FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards
and Technology of the United States
of America

FIPS VALIDATED 140-2 ™

The Communications Security
Establishment of the Government
of Canada

Consolidated Certificate No. 0039

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions, Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature: Michael J Cooper

Dated: 4/2/2014

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 2 April 2014.

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

TM A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2096	3/5/2014	WatchDox(R) CryptoModule	WatchDox, Inc.	Software Version: 1.0
2097	3/5/2014	RSA BSAFE(R) Crypto-C Micro Edition	RSA, The Security Division of EMC	Software Version: 4.0.1
2098	3/5/2014	IDPrime MD 830	Gemalto	Hardware Version: SLE78CFX3009P; Firmware Version: IDCore30 Build 1.17, IDPrime MD Applet version V4.1.2.F and MSPNP Applet V1.0
2099	3/7/2014	Riverbed Cryptographic Security Module	Riverbed Technology, Inc.	Software Version: 1.0
2100	3/7/2014	Cisco FIPS Object Module	Cisco Systems, Inc.	Software Version: 4.1
2101	03/14/2014	Symantec App Center Server Cryptographic Module	Symantec Corporation	Software Version: 1.0
2102	03/11/2014	Juniper Networks EX6200 and EX8200 Ethernet Switches Routing Engines	Juniper Networks, Inc.	Hardware Versions: EX6200-SRE64-4XS, EX8208-SRE320 and EX8216-RE320 with Tamper Evident Labels: 520-052564; Firmware Version: JUNOS 12.1R6.6
2103	03/14/2014	ProtectServer Gold (PSG)	SafeNet, Inc.	Hardware Versions: B2, B3, B4 and PSG-01-0101; Firmware Version: 3.20.01
2104	03/18/2014	NSA E7500	Dell SonicWALL	Hardware Version: P/N 101-500226-54, Rev. A; Firmware Version: SonicOS v5.9.0
2105	03/19/2014	FortiAnalyzer 4.0 MR3	Fortinet, Inc.	Firmware Version: v4.0, build3059, 130918
2106	03/19/2014	M3-SE-RTR2 and TXC3	DTECH LABS, Inc.	Hardware Versions: M3-SE-RTR2-FIPS and TXC3-FIPS with DT-FIPS-TEL; Firmware Version: 15.2(2)GC
2107	03/19/2014	Vocera Cryptographic Module	Vocera Communications, Inc.	Hardware Version: 88W8688; Software Version: 2.1; Firmware Version: 2.0

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2108	03/19/2014	OpenPeak Cryptographic Security Module	OpenPeak, Inc.	Software Version: 1.0
2109	03/21/2014	Odyssey Security Component Kernel Mode	Juniper Networks, Inc	Software Version: 2.50
2110	03/21/2014	BlackBerry Cryptographic Library for Secure Work Space	BlackBerry Ltd.	Software Version: 1.0
2111	03/21/2014	Christie IMB-S2 4K Integrated Media Block (IMB)	Christie Digital Systems Canada, Inc.	Hardware Version: 000-102675-01; Firmware Versions: 1.0.1-2641, 1.0.3-3047, 1.1.0-3271, 1.2.0-3400, 1.2.1-3546, 1.3.0-3704 or 1.3.2-3709
2112	03/25/2014	AT&T Toggle Cryptographic Security Module	AT&T Services, Inc.	Software Version: 1.0
2113	03/25/2014	FortiGate-VM Virtual Appliances	Fortinet, Inc.	Software Version: 4.0 MR3
2114	3/26/2014	Proofpoint Security Library	Proofpoint Incorporated	Software Version: 2.0
2115	03/26/2014	FortiAnalyzer-4000B	Fortinet, Inc.	Hardware Version: 4000-B with SKU-FIPS-SEAL-RED; Firmware Version: v4.0, build3059, 130918

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2116	3/26/2014	Cisco Catalyst 4503-E, Catalyst 4506-E, Catalyst 4507R-E, Catalyst 4507R+E, Catalyst 4510R-E, Catalyst 4510R+E, Catalyst C4500X-16SFP+, Catalyst C4500X-F-16SFP+, Catalyst C4500X-32SFP+, Catalyst C4500X-F-32SFP+, Catalyst C4500X-24X-ES, Catalyst C4500X-40X-ES, Catalyst C4500X-24X-IPB with Supervisor Cards (WS-X45-SUP7-E, WS-X45-Sup7L-E) and Line Cards (WS-X4640-CSFP-E, WS-X4712-SFP+E, WS-X4748-NGPOE+E, WS-X4748-RJ45-E and WS-X4748-RJ45V+E)	Cisco Systems, Inc.	Hardware Version: Catalyst 4503-E [1, 3, 4, 5, 6, 8, A], Catalyst 4503-E [2, 5, 7, 8, A], Catalyst 4506-E [1, 3, 4, 5, 6, 7, 8, B], Catalyst 4506-E [2, 3, 4, 5, 6, 7, 8, B], Catalyst 4507R-E [1, 3, 4, 5, 6, 7, 8, C], Catalyst 4507R-E [2, 3, 4, 5, 6, 7, 8, C], Catalyst 4507R+E [1, 3, 4, 5, 6, 7, 8, C], Catalyst 4507R+E [2, 3, 4, 5, 6, 7, 8, C], Catalyst 4510R-E [1, 3, 4, 5, 6, 7, 8, D], Catalyst 4510R+E [1, 3, 4, 5, 6, 7, 8, D], Catalyst C4500X-16SFP+ [E], Catalyst C4500X-F-16SFP+ [E], Catalyst C4500X-32SFP+ [E], Catalyst C4500X-F-32SFP+ [E], Catalyst C4500X-24X-ES [E], Catalyst C4500X-40X-ES [E], Catalyst C4500X-24X-IPB [E], Supervisor Card WS-X45-SUP7-E [1], Supervisor Card WS-X45-SUP7L-E [2], Line Card WS-X4748-RJ45V+E [3], Line Card WS-X4712-SFP+E [4], Line Card WS-X4640-CSFP-E [5], Line Card WS-X4748-NGPOE+E [6], Line Card WS-X4748-RJ45-E [7], Filler Plate (C4K-SLOT-CVR-E) [8] and FIPS kit packaging (WS-C4503-FIPS-KIT= [A], WS-C4506-FIPS-KIT= [B], WS-C4507-FIPS-KIT= [C], WS-C4510-FIPS-KIT= [D] and CVPN4500FIPS/KIT= [E]); Firmware Version: IOS-XE 3.5.0E

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2117	3/28/2014	Juniper Networks EX3300, EX4200, EX4500 Ethernet Switches	Juniper Networks, Inc.	Hardware Version: EX3300-24P, EX3300-24T, EX3300-24T-DC, EX3300-48T, EX3300-48T-BF, EX3300-48P, EX4200-24P, EX4200-24PX, EX4200-24T, EX4200-24F, EX4200-48P, EX4200-48PX, EX4200-48T, EX4500-40-FB and EX4500-40-BF with Tamper Evident Labels: 520-052564; Firmware Version: JUNOS 12.1R6.6
2119	3/28/2014	Seagate Secure® TCG Opal SSC Self-Encrypting Drive FIPS 140-2 Module	Seagate Technology LLC	Hardware Version: 1G1162 and 1G1164; Firmware Version: SM72, DM72, DM82, HM72, HM82 and LM72
2120	3/28/2014	Samsung OpenSSL Cryptographic Module	Samsung Electronics Co., Ltd.	Software Version: SecOpenSSL2.0.3